Testimony of Dr. Dan S. Wallach
Senate Elections, Reapportionment & Constitutional Amendments Committee
February 16, 2006

Thank you very much for holding today's hearings. I appreciate the opportunity to speak to you today about the security issues in the electronic voting systems that are increasingly being used in the U.S.

I am an associate professor in the department of computer science at Rice University in Houston, Texas. I earned my bachelor's degree at the University of California, Berkeley in 1993 and my doctorate degree at Princeton University in 1999. I study computer security and have published over forty refereed academic papers on computer security and related topics[1]. In general, I look at computer security as an engineering problem. The goal in designing and building a secure system is to understand the threats the system might face and to build in appropriate safeguards to protect against those threats.

I have studied security issues in electronic voting since 2001, when Houston became an early adopter of these systems. In 2003, I co-authored a study with Adam Stubblefield, Tadayoshi Kohno, and Aviel Rubin, at Johns Hopkins University, that examined the design of the Diebold AccuVote-TS voting system; that paper appeared at an IEEE security conference. I am presently the associate director of ACCURATE[2] (A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections), an NSF-funded center spanning six institutions which is studying software architectures, tamper-resistant hardware, cryptographic protocols and verification systems as applied to electronic voting systems. Additionally, ACCURATE will examine system usability and how public policy, in combination with technology, can better safeguard voting nationwide.

I was invited here today to discuss the adequacy of the present testing and certification process for voting systems. Testing and certification are always done with respect to *standards*, so any discussion of testing must consider what, exactly, is required to be tested. Recently, the EAC and NIST finalized their voting machine standards (VVSG)[3]. These 2005 "voluntary" standards are meant to supplant the 2002 standards that many states have adopted. While the 2005 standards are a significant improvement over earlier standards, they still have very little to say about critical issues that may effect vulnerabilities in voting systems. In particular, there is no significant attention paid to the engineering process (software and hardware) used to create voting systems. Building reliable and secure software is radically more difficult than simply building software that "works." For critical applications, such as airplane controls, the software engineering process, itself, is carefully designed to minimize the inclusion of errors. *At present, no voting standards make any requirements on software engineering processes*. The results were predictable. When California discovered many of its Diebold voting systems to be running uncertified versions of the software, the problem was one of a lack of process. When we had the chance to read Diebold's source code, what we saw was clearly the result of an ad-hoc development environment. Diebold's developers made naïve mistakes and, simply, did not have any concept of the threats that a voting system must be engineered to face.

A significant part of the problem is that the voting system standards represent a single bar for a vendor to hurdle. As a result of vendor pressures in the standards process, this bar has been set to an embarrassingly low level. An important first step is to replace this with a multi-level evaluation, as is done with other security standards such as the Common Criteria (used to evaluate a variety of other security devices). Rather than getting a single thumbs-up or thumbs-down, a voting system should instead get a number grade across many different aspects (e.g., software security, hardware reliability, usability/accessibility, and so forth) with a minimum defined for each. This gives vendors a competitive incentive to go above and beyond the minimum requirements.

California could, for example, define the 2005 VVSG as its baseline and then define more stringent standards above this, including usability concerns, software engineering concerns, and other techniques such as voter verifiable paper audit trails (VVPAT). Where the VVSG merely suggests how vendors might choose to implement VVPAT, if they desire, California should give higher grades to better implementations. For example, voting machines that print the votes on continuous paper rolls should score lower; because the paper roll has the

[1] `http://www.cs.rice.edu/~dwallach/pubs.html`
[2] `http://accurate-voting.org`
[3] `http://www.eac.gov/vvsg_intro.htm`

votes recorded in the order they were cast, it becomes much easier to violate a voter's anonymity. Numeric grading would also influence voting system procurements, allowing the purchase of systems today whose vendors contractually promise improvements tomorrow. This could bridge the gap between where we are today and where we want to be tomorrow.

An interesting question is whether California could jump-start the process by changing the business model for voting system vendors. Presently, a vendor will typically sell or lease a comprehensive system to a county, where the county will be unable to mix in equipment from other vendors. This creates "lock-in" and its associated expenses. Even if a competitive vendor offers a clearly superior product, the financial and procedural costs to change vendors may be prohibitive. As an alternative, California could define interoperable hardware standards for voting systems, analogous to the standards for personal computers, where vendors compete to sell hardware that run standard software. By divorcing the software from the hardware, each market will become more competitive and lower cost. A county may switch software on its existing hardware, or it may mix hardware from a new vendor with its existing machines.

Finally, a critical aspect of any voting system is its *transparency*. Existing, proprietary voting systems are not auditable by third parties. We were only able to audit Diebold's software because they accidentally leaked it on the Internet. Third-party auditing, sometimes called "Red Team" or "Tiger Team" exercises, are critical to gain confidence in a system's security. Such analyses, performed on behalf of the states of Maryland and Ohio, have found significant issues in every voting system they have ever examined. While companies should be required to pay for these analyses, the states should be able to choose the 3rd party expert examiners to guarantee that companies do not simply shop around for analysts willing to rubber-stamp their systems. While such audits may be conducted in private, there's no reason they may not also be conducted in public. Trade secrets have no place in election systems. Voting system vendors may feel free to assert copyright or patent rights on their products, but they should be compelled to disclose the inner workings of their products to the public. While such disclosure may make it somewhat easier for "bad guys", it also makes it easier for "good guys" (and, we generally assume that the "bad guys" already have insider knowledge of how these systems work). Increased transparency will be necessary, in the end, to convince the electorate that your other regulatory steps are working as you intended.